PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 : H04Q 7/38

A1

(11) Internationale Veröffentlichungsnummer: WO 99/33299

(43) Internationales Veröffentlichungsdatum: 1. Juli 1999 (01.07.99)

(21) Internationales Aktenzeichen: PCT/DE98/03545

(22) Internationales Anmeldedatum: 2. Dezember 1998 (02.12.98)

(30) Prioritätsdaten:
197 56 587.5 18. Dezember 1997 (18.12.97) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D–80333 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: MENZEL, Christian [DE/DE]; Edelweissstrasse 36, D–82216 Maisach (DE). HAFERBECK, Ralf [DE/DE]; St.–Benedikt–Strasse 5, D–85716 Unterschleissheim (DE).

(74) Gemeinsamer Vertreter: SIEMENS AKTIENGESELLSCHAFT; Postfach 22 16 34, D–80506 München (DE).

(81) Bestimmungsstaaten: CN, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

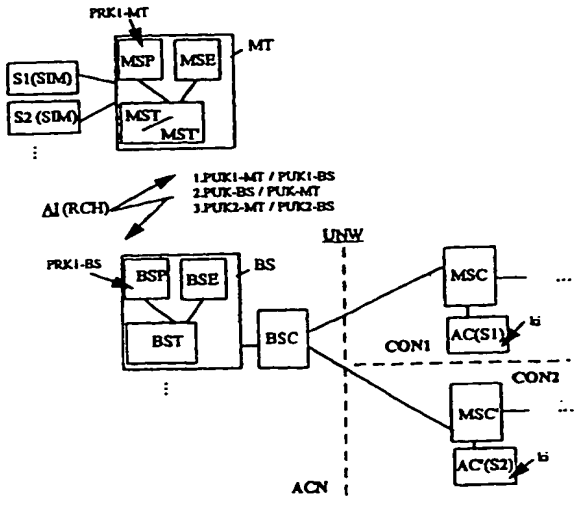
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND COMMUNICATIONS SYSTEM FOR CIPHERING INFORMATION FOR A RADIO TRANSMISSION AND FOR AUTHENTICATING SUBSCRIBERS

(54) Bezeichnung: VERFAHREN UND KOMMUNIKATIONSSYSTEM ZUR VERSCHLÜSSELUNG VON INFORMATIONEN FÜR EINE FUNKÜBERTRAGUNG UND ZUR AUTHENTIFIKATION VON TEILNEHMERN

(57) Abstract

The invention relates to a method and a communications system for ciphering information for a radio transmission in an access network (ACN), and for carrying out an authentication in at least one core network (CON1, CON2). According to the invention, public keys (PUK1–MT, PUK–BS) are transmitted alternately between a mobile station (MT) and the base station (BS) via a radio interface (AI). The public key (PUK1–MT or PUK–BS) received by the base station (BS) or mobile station (MT) is used for ciphering the information which is to be subsequently transmitted via the radio interface. The enciphered information received by the mobile station or base station can be deciphered using a private key (PRK1–MT, PRK1–BS) allocated to the public key (PUK1–MT, PUK–BS) in the mobile station or the base station (BS). Following the ciphering procedure, the respective core network (CON1, CON2) is authenticated by a mobile radio specific device (SIM) of the mobile station and the subscriber is authenticated by a device (AC, AC') of the core network, using alternately transmitted enciphered information.



(57) Zusammenfassung

Der Gegenstand der Erfindung geht von einer Verschlüsselung der Informationen für die Funkübertragung in einem Zugangsnetz (ACN) sowie einer Authentifikation in zumindest einem Kernnetz (CON1, CON2) aus. Erfindungsgemäss werden zwischen einer Mobilstation (MT) und der Basisstation (BS) über die Funkschnittstelle (AI) wechselseitig öffentliche Schlüssel (PUK1–MT, PUK–BS) gesendet, und der von der Basisstation (BS) bzw. Mobilstation (MT) empfangene öffentliche Schlüssel (PUK1–MT bzw. PUK–BS) zur Verschlüsselung der nachfolgend über die Funkschnittstelle zu sendenden Informationen verwendet. Anhand eines privaten Schlüssels (PRK1–MT, PRK1–BS), der dem gesendeten öffentlichen Schlüssel (PUK1–MT, PUK–BS) in der Mobilstation (MT) bzw. in der Basisstation (BS) zugeordnet ist, können die von der Mobilstation bzw. Basisstation empfangenen verschlüsselten Informationen entschlüsselt werden. Im Anschluss an die Verschlüsselungsprozedur werden von einer mobilfunkspezifischen Einrichtung (SIM) der Mobilstation die Authentifikation des jeweiligen Kernnetzes (CON1, CON2) und von einer Einrichtung (AC, AC') des Kernnetzes die Authentifikation des Teilnehmers anhand wechselseitig gesendeter verschlüsselter Informationen durchgeführt.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Beschreibung

Verfahren und Kommunikationssystem zur Verschlüsselung von Informationen für eine Funkübertragung und zur Authentifikation von Teilnehmern

Die Erfindung betrifft ein Verfahren zur Verschlüsselung von Informationen für eine Funkübertragung und zur Authentifikation von Teilnehmern in einem Kommunikationssystem, sowie ein entsprechendes Kommunikationssystem.

Kommunikationssysteme, wie beispielsweise das Mobilfunksystem nach dem GSM-Standard (Global System for Mobile Communication), nutzen zur drahtlosen Informationsübertragung eine Funkschnittstelle, auf der Verbindungen zwischen Mobilstationen und Basisstationen eines Mobilfunknetzes aufgebaut, abgebaut und aufrechtgehalten werden können. Aus dem Aufsatz „Safety First bei europaweiter Mobilkommunikation", telcom report 16 (1993), Heft 6, Seiten 326 bis 329, ist ein Verfahren und ein System zur Verschlüsselung (ciphering) von Informationen für die Funkübertragung und zur Teilnehmerauthentifikation bekannt. Dabei identifizieren sich die mobilen Teilnehmer mit einer Einrichtung - auch als Teilnehmeridentitätsmodul oder SIM-Karte (Subscriber Identity Module) bezeichnet -, das in der Funkteilnehmerstation enthalten ist, gegenüber dem Mobilfunknetz. Der mobile Teilnehmer wird netzseitig in einer Einrichtung - z.B. einer Authentifikationseinrichtung (Authentification Center) - registriert, von der zum Schutz der Teilnehmerdaten der mobilen Teilnehmer jeweils Sicherheitsparameter und Sicherheitsalgorithmen bereitgestellt werden. Die Verschlüsselung der Informationen auf der Funkschnittstelle erfolgt teilnehmerbezogen, und ist mit der Teilnehmerauthentifikation unmittelbar gekoppelt.

In zukünftigen Kommunikationssystemen - wie z.B. einem universellen Netz (UMTS, Universal Mobile Telecommunication System, oder UPT, Universal Personal Telecommunication) - be-

steht die Tendenz, die Infrastruktur in ein Zugangsnetz (Access Network) und ein oder mehrere Kernnetze (Core Networks) zu unterteilen. Der Bereich des Zugangsnetzes ist dabei für Angelegenheiten der Funkschnittstelle - wie Verwaltung und Zuteilung der Funkkanäle, Kanalkodierung, Verschlüsselung über die Funkschnittstelle usw. - zuständig, wohingegen der Bereich des Kernnetzes hauptsächlich für Angelegenheiten der Teilnehmerverwaltung - wie Registrierung (Subscription), Authentifikation, Auswahl des Zugangsnetzes usw. - sowie für die Bereitstellung von Diensten verantwortlich ist. Eine Verschlüsselung der Informationen für die Funkübertragung unabhängig vom Kernnetz ist beim derzeitigen GSM-System unmöglich. Darüber hinaus wird eine Funkressource - z.B. der Funkkanal - exclusiv nur für einen Teilnehmer, nämlich den Teilnehmer, der gerade authentifiziert wurde, beim Verschlüsseln benutzt, was in zukünftigen Kommunikationssystemen insbesondere bei gleichzeitiger Nutzung einer Mobilstation durch mehrere Teilnehmer (z.B. durch ihre SIM-Karten) nicht mehr ausreicht.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren und ein Kommunikationssystem anzugeben, das eine Verschlüsselung der Informationen auf der Funkschnittstelle unabhängig von Art und Anzahl der Kernnetze ermöglicht, sodaß sich eine funktionale Trennung von Verschlüsselung und Authentifikation ergibt.

Diese Aufgabe wird gemäß der Erfindung durch das Verfahren mit den Merkmalen des Patentanspruchs 1 und durch das Kommunikationssystem mit den Merkmalen des Patentanspruchs 12 gelöst. Weiterbildungen der Erfindung sind den Unteransprüchen zu entnehmen.

Der Gegenstand der Erfindung geht von einer Verschlüsselung der Informationen für die Funkübertragung in einem Zugangsnetz sowie einer Authentifikation in zumindest einem Kernnetz aus. Erfindungsgemäß werden zwischen einer Mobilstation, die

von mehreren Teilnehmern parallel nutzbar ist, und der Basisstation über die Funkschnittstelle wechselseitig öffentliche Schlüssel gesendet, und der von der Basisstation bzw. Mobilstation empfangene öffentliche Schlüssel zur Verschlüsselung der nachfolgend über die Funkschnittstelle zu sendenden Informationen verwendet. Anhand eines privaten Schlüssels, der dem gesendeten öffentlichen Schlüssel in der Mobilstation bzw. in der Basisstation zugeordnet ist, können die von der Mobilstation bzw. Basisstation empfangenen verschlüsselten Informationen entschlüsselt werden. Im Anschluß an die Verschlüsselungsprozedur werden von einer Einrichtung der Mobilstation die Authentifikation des jeweiligen Kernnetzes und von der Einrichtung des Kernnetzes die Authentifikation des Teilnehmers anhand wechselseitig gesendeter verschlüsselter Informationen durchgeführt.

Durch das gegenseitige Übertragen von öffentlichen Schlüsseln zwischen Mobilstation und Basisstation kann die Verschlüsselung für die Funkübertragung nicht teilnehmerbezogen, sondern mobilstationsbezogen - und damit für mehrere Teilnehmer gleichzeitig - erfolgen. Es besteht eine bidirektionale vertraute Verbindung (trusted relationship), in die sich eine „Schein"-Basisstation oder eine nicht authorisierte Basisstation nicht einschalten kann. Ein weiterer Vorteil ist die funktionale Trennung von Zugangsnetz - verantwortlich für Verschlüsselung - und Kernnetz - verantwortlich für Authentifikation. Die Funkressource wird mehrfach ausgenutzt für die Verschlüsselung mehrerer Teilnehmer an der Mobilstation. Die für die Authentifikationsprozedur erforderlichen Informationen können bereits verschlüsselt übertragen werden, was im bisherigen GSM-System nicht möglich ist. Maximale Sicherheit wird durch die Kombination der Verschlüsselung mit öffentlichen/rivaten Schlüsseln auf Mobilstationsebene und der nachfolgenden Authentifikation auf Teilnehmerebene erreicht. Insbesondere können durch die funktionale Trennung von Zugangsnetz und Kernnetz an das Zugangsnetz gleichzeitig mehrere Kernnetze - gegebenenfalls unterschiedlicher Netzart - paral-

lel angeschaltet sein, und insbesondere mehrere Teilnehmer mit verschiedenen Identitäten (SIM-Karten) gleichzeitig über eine Mobilstation und in verschiedenen Kernnetzen kommunizieren.

In die sichere Verbindung, erreicht durch mehrfaches gegenseitiges Übertragen der öffentlichen Schlüssel, kann sich kein Dritter nachträglich einschleichen. Durch die anschließende Authentifikation ist gewährleistet, daß die jeweilige Gegeneinrichtung der Verbindung - d.h. die Basisstation aus Sicht der Mobilstation bzw. die Mobilstation aus Sicht der Basisstation - auch wirklich die Einrichtung ist für die sich zu Beginn der Kommunikations ausgegeben hat.

Eine vorteilhafte Weiterbildung der Erfindung sieht vor, daßzunächst von der Mobilstation ein erster öffentlicher Schlüssel zur Basisstation gesendet wird, die ihn zur Verschlüsselung der Informationen verwendet, und von der Basisstation ein öffentlicher Schlüssel zur Mobilstation gesendet wird, die ihn zur Verschlüsselung der Informationen verwendet. Danach sendet die Mobilstation einen zweiten öffentlichen Schlüssel zur Basisstation. Damit wird das Einschalten einer „Schein"-Basisstation oder der nicht authorisierten Basisstation in die Verbindung auf der Funkschnittstelle sicher verhindert. Vorzugsweise ersetzt dabei der zweite Schlüssel den ersten Schlüssel.

Gemäß einer alternativen Weiterbildung der Erfindung sendet zunächst die Basisstation einen ersten öffentlichen Schlüssel zur Mobilstation, die ihn zur Verschlüsselung der Informationen verwendet, sowie die Mobilstation einen öffentlichen Schlüssel zur Basisstation, die ihn zur Verschlüsselung der Informationen verwendet. Danach wird von der Basisstation ein zweiter öffentlicher Schlüssel zur Mobilstation gesendet. Damit wird das Einschalten der „Schein"-Basisstation oder der nicht authorisierten Basisstation in die Verbindung auf der

Funkschnittstelle sicher verhindert. Vorzugsweise wird dabei der zweite Schlüssel durch den ersten Schlüssel ersetzt.

Von Vorteil ist es gemäß einer anderen Weiterbildung der Erfindung, daß von der Mobilstation eine Teilnehmeridentität des Teilnehmers und eine Authentifikationsanforderung an das Kernnetz verschlüsselt gesendet und von einer Einrichtung des Kernnetzes eine Authentifikationsantwort verschlüsselt rückgesendet wird. Daraufhin wird von der Mobilstation eine Authentifikationsprozedur zur Überprüfung der Identität des Kernnetzes ausgeführt. Damit erfolgt mobilstationsseitig eine Netzauthentifikation, was insbesondere bei mehreren Kernnetzen in Abhängigkeit davon, wo der Teilnehmer registriert ist, individuell ausgeführt werden kann.

Vorzugsweise wird von der Einrichtung des Kernnetzes eine Authentifikationsanforderung zusätzlich zu der Authentifikationsantwort verschlüsselt gesendet und von der Mobilstation eine Authentifikationsantwort an die Einrichtung verschlüsselt rückgesendet. Daraufhin kann von der Einrichtung des Kernnetzes eine Authentifikationsprozedur zur Überprüfung der Teilnehmeridentität ausgeführt werden. Dies hat den Vorteil, daß mit der Antwort der Netzeinrichtung auf die Netzauthentifikation die Anforderung zur Überprüfung der Teilnehmerauthentifikation mitgesendet und von der Netzeinrichtung unmittelbar bei Eintreffen der Antwort veranlaßt werden kann.

Ein Kommunikationssystem gemäß der Erfindung weist Speichereinrichtungen in einer Mobilstation, die von mehreren Teilnehmern parallel nutzbar ist, und in der Basisstation zum Speichern öffentlicher Schlüssel und privater Schlüssel, die den öffentlichen Schlüsseln zugeordnet sind, auf. Sendeeinrichtungen in der Mobilstation und in der Basisstation sorgen für das wechselseitige Senden der öffentlichen Schlüssel über die Funkschnittstelle. Steuereinrichtungen in der Mobilstation und in der Basisstation sind zur Verschlüsselung der nachfolgend über die Funkschnittstelle zu sendenden Informa-

tionen unter Verwendung der von der Basisstation bzw. Mobilstation empfangenen öffentlichen Schlüssel und zur Entschlüsselung der empfangenen verschlüsselten Informationen anhand des gespeicherten zugehörigen privaten Schlüssels vorgesehen. Darüber hinaus weist das Kommunikationssystem eine teilnehmerspezifische Einrichtung in der Mobilstation und eine Steuereinrichtung im jeweiligen Kernnetz zur Durchführung der Authentifikation des Kernnetzes sowie der Authentifikation der Teilnehmer anhand wechselseitig gesendeter verschlüsselter Informationen auf.

Im folgenden wird die Erfindung anhand eines Ausführungsbeispiels bezugnehmend auf zeichnerische Darstellungen näher erläutert.

Dabei zeigen

FIG 1 das Blockschaltbild eines Kommunikationssystems mit einem Zugangsnetz für die Funkübertragung und mehreren Kernnetzen für die Authentifikation,

FIG 2 den Nachrichtenfluß für die Verschlüsselung der Informationen auf der Funkschnittstelle zwischen einer Mobilstation und einer Basisstation des Zugangsnetzes, und

FIG 3 den Nachrichtenfluß für die Authentifikation der Teilnehmer und der Kernnetze zwischen der Mobilstation und einer Netzeinrichtung des jeweiligen Kernnetzes.

Das in FIG 1 dargestellte Kommunikationssystem ist ein Kommunikationssystem UNW - wie z.B. ein universelles UMTS- oder UPT-Netz (Universal Mobile Telecommunication System oder Universal Personal Telecommunication) -, deren Infrastruktur in ein Zugangsnetz ACN (Access Network) und in ein oder mehrere Kernnetze CON1, CON2 (Core Networks) unterteilt ist. Der Be-

reich des Zugangsnetzes ACN mit Einrichtungen eines Funkteilsystems - wie z.B. Basisstationen BS und daran angeschlossene Basisstationssteuerungen BSC - ist dabei für Angelegenheiten der Funkschnittstelle, wie Verwaltung und Zuteilung von Funkkanälen, Kanalkodierung, Verschlüsselung über die Funkschnittstelle usw. - zuständig. Der Bereich des Kernnetzes CON1, CON2 mit Netzeinrichtungen - wie z.B. Vermittlungseinrichtung MSC, MSC' und Authentifikationseinrichtung AC, AC' - ist hauptsächlich für Angelegenheiten des Routings, der Teilnehmerverwaltung, wie Registrierung (Subscription) der Teilnehmer S1, S2 sowie Authentifikation, Auswahl des Zugangsnetzes ACN usw., und für die Bereitstellung von Diensten verantwortlich. Die Authentifikationsprozeduren in den Einrichtungen AC, AC' benutzen vorzugsweise geheime Schlüssel ki gemäß der bekannten Vorgehensweise nach GSM-Standard, um die Teilnehmerauthentifikation für den im Kernnetz CON1 registrierten Teilnehmer S1 und für den im Kernnetz CON2 registrierten Teilnehmer S2 parallel und unabhängig vom Zugangsnetz ACN auszuführen.

Beide Vermittlungseinrichtungen MSC, MSC' in den Kernnetzen CON1 und CON2 sind im vorliegenden Beispiel an die Basisstationssteuerung BSC des Zugangsnetzes ACN angeschlossen. Die Basisstationssteuerung BSC ermöglicht die Verbindung zu mindestens einer Basisstation, im vorliegenden Beispiel zu der Basisstationen BS. Eine solche Basisstation BS ist eine Funkstation, die zur Abdeckung eines Funkbereichs - z.B. einer Funkzelle - angeordnet ist, um über eine Funkschnittstelle AI Verbindungen von/zu mindestens einer Mobilstation MT, die sich in ihrem Funkbereich aufhält, aufbauen, abbauen und aufrechthalten zu können. Die Informationen sind dabei in einem von der Basisstationssteuerung BSC zugeteilten Funkkanal RCH enthalten. Bei den Verbindungen kann es sich sowohl um abgehende als auch um ankommende Verbindungen handeln. Die Mobilstation MT eignet sich im vorliegenden Beispiel besonders zur gleichzeitigen Nutzung durch mehrere Teilnehmer S1 und S2, die durch ihre teilnehmerspezifischen Einrichtungen SIM

(Subscriber Identity Module) an einem - nicht dargestellten - internen Bus parallel hängen und jeweils eine eigene Teilnehmeridentität haben.

Die Mobilstation MT weist eine Speichereinrichtung MSP, eine Sende- und Empfangseinrichtung MSE sowie Steuereinrichtungen MST, MST', die mit Speichereinrichtung MSP und Sende- und Empfangseinrichtung MSE verbunden sind, auf. Ebenso weist die Basisstation BS eine Speichereinrichtung BSP, eine Sende- und Empfangseinrichtung BSE sowie eine Steuereinrichtung BST, die mit Speichereinrichtung BSP und Sende- und Empfangseinrichtung BSE verbunden ist, auf.

Gemäß der Erfindung sendet die Mobilstation MT - stationsbezogen über die Sende- und Empfangseinrichtung MSE - für alle an ihr aktiven Teilnehmer parallel einen ersten öffentlichen Schlüssel PUK1-MT (public key) über die Funkschnittstelle AI aus und merkt sich einen dazugehörigen privaten Schlüssel PRK1-MT (private key), der in der Speichereinrichtung MSP oder in der Steuereinrichtung MST abgelegt ist. Die Basisstation BS verwendet den empfangenen öffentlichen Schlüssel PUK1-MT zur Verschlüsselung der nachfolgend über die Funkschnittstelle AI zu sendenden Informationen. Das Entschlüsseln der von der Basisstation BS gesendeten Informationen ist damit nur der Einrichtung möglich, die den zugehörigen privaten Schlüssel kennt, d.h. der Mobilstation MT mit dem Schlüssel PRK1-MT. In der Antwort der Basisstation BS sendet sie ihrerseits einen öffentlichen Schlüssel PUK-BS in der Gegenrichtung zur Mobilstation MT und merkt sich den dazugehörigen privaten Schlüssel PRK1-BS. Den privaten Schlüssel PRK1-BS speichert die Speichereinrichtung BSP oder die Steuereinrichtung BST. Damit ist sichergestellt, daß auch im folgenden von der Mobilstation MT an die Basisstation BS gesendete Informationen, die unter Verwendung des öffentlichen Schlüssels PUK-BS verschlüsselt sind, nur von der Basisstation BS bzw. deren Steuereinrichtung BST wieder entschlüsselt werden können.

Um zu verhindern, daß eine „Schein"-Basisstation oder nicht authorisierte Basisstation den von der Mobilstation MS übermittelten öffentlichen Schlüssel PUK1-MT zum Senden korrekt verschlüsselter Informationen - zufällig oder absichtlich - benutzen kann, sendet die Mobilstation MT einen zweiten öffentlichen Schlüssel PUK2-MT - bereits verschlüsselt - über die Funkschnittstelle AI zur Basisstation BS. Diesen Schlüssel PUK2-MT kann nur die richtige Basisstation BS, mit der eine vertrauliche Verbindung auf Mobilstationsebene anfangs aufgebaut wurde, lesen und verwenden. Die Schein"-Basisstation oder nicht authorisierte Basisstation ist auf diese sicher ausgeschaltet. Dabei ersetzt der zweite öffentliche Schlüssel PUK2-MT den bisherigen ersten öffentlichen Schlüssel PUK1-MT. Gleiches gilt für die andere Übertragungsrichtung, wenn die gegenseitige Übertragung der Schlüssel von der Basisstation BS initiiert wird.

Die Verschlüsselungsprozedur kann ebenso von der Basisstation BS initiiert werden, sodaß zunächst von der Sende- und Empfangseinrichtung BSE ein erster öffentlicher Schlüssel PUK1-BS, dem ein privater Schlüssel PRK1-BS zugeordnet und in der Steuereinrichtung BST oder der Speichereinrichtung BSP gespeichert ist, zur Mobilstation MT gesendet wird. Diese verwendet den eintreffenden öffentlichen Schlüssel PUK1-BS zur Verschlüsselung der nachfolgenden Informationen und sendet ihrerseits einen öffentlichen Schlüssel PUK-MT zur Basisstation BS, die ihn zur Verschlüsselung der Informationen in der Gegenrichtung verwendet. Anschließend sendet die Basisstation BS vorzugsweise einen zweiten öffentlichen Schlüssel PUK2-BS zur Mobilstation MT, um ganz sicherzugehen, daß sich nicht eine unerwünschte Basisstation in die verschlüsselte Informationsübertragung über den Funkkanal einmischt oder diese abhört. Die öffentlichen wie die privaten Schlüssel bestehen beispielsweise aus einer Zahlenfolge oder Bitfolge.

Im Anschluß an die Verschlüsselungsprozedur werden von der Mobilstation MT - vorzugsweise von der nur zur Authentifikation vorgesehenen Einrichtung SIM oder auch von einer für Verschlüsselung und Authentifikation gemeinsam zuständigen Steuereinrichtung MST - die Authentifikation des jeweiligen Kernnetzes CON1, CON2 und von der Einrichtung AC, AC' des Kernnetzes CON1, CON2 die Authentifikation des Teilnehmers S1, S2 anhand wechselseitig gesendeter verschlüsselter Informationen auf Teilnehmerebene durchgeführt (siehe Figur 3). Die bidirektionale Authentifikation läuft damit unabhängig vom Zugangsnetz ACN ab. Die an die Verschlüsselung angehängte Authentifikation stellt maximale Sicherheit bereit, da sie gewährleistet, daß die Gegeneinrichtung der Verbindung wirklich die Einrichtung ist, für die sie sich zu Beginn der Kommunikation ausgegeben hat. Damit wird verhindert, daß die gesamte Kommunikation auf dieser Verbindung von einer Schein"-Basisstation oder nicht authorisierten Basisstation initiiert wurde. Ein weiterer Vorteil der funktionalen Trennung von Verschlüsselung und Authentifikation besteht darin, daß die Teilnehmeridentitäten und die für die Authentifikation erforderlichen Informationen - z.B. Zufallszahl RAND, Antwortsignal SRES (Signed Response) gemäß GSM-Verfahren - bereits verschlüsselt über die Funkschnittstelle AI übertragen werden können. Zur Authentifikation können auch vom GSM-Verfahren abweichende Authentifikationsprozeduren verwendet werden.

An das Zugangsnetz ACN können parallel mehrere Kernnetze - im vorliegenden Beispiel die beiden Kernnetze CON1, CON2 - auch unterschiedlicher Netzart angeschlossen sein. Die Teilnehmer S1, S2 arbeiten mit verschiedenen SIM-Karten gleichzeitig über die eine Mobilstation MT in verschiedenen Kernnetzen - im vorliegenden Beispiel in den beiden Kernnetzen CON1, CON2 - bzw. ein oder mehrere Teilnehmer S1, S2 in einem einzigen Kernnetz, z.B. CON1. Ferner unterstützt die funktionale Trennung von Zugangsnetz ACN und Kernnetz CON1, CON2 auch Konfigurationen, bei denen das Zugangsnetz ACN und das oder die

Kernnetze CON1, CON2 unterschiedliche Netzbetreiber aufweisen.

Figur 2 zeigt in schematischer Darstellung den Nachrichtenfluss zur Verschlüsselung der Informationen für die Funkübertragung zwischen der Mobilstation MT und der Basisstation BS des Zugangsnetzes. Dabei ist das Beispiel darauf beschränkt, daß der gegenseitige Austausch der Schlüssel von der Mobilstation MT initiiert wird. Ebenso könnte die Basisstation BS den Austausch beginnen (siehe auch Beschreibung zu Figur 1), der nachfolgende Nachrichtenfluß liefe in entsprechender Weise ab.

Nach der Zuteilung des Funkkanals RCH für einen Verbindungsaufbau zur Kommunikation startet die Mobilstation MT die Verschlüsselung, in dem sie in einer Nachricht SEND den öffentlichen Schlüssel PUK1-MT aussendet und sich den zugehörigen privaten Schlüssel PRK1-MT merkt. Damit hat die verschlüsselte Übertragung von Informationen auf der Funkschnittstelle begonnen. Die Basisstation BS benutzt den eintreffenden Schlüssel PUK1-MT zur verschlüsselten Informationsübertragung in der Gegenrichtung, und sendet ihrerseits den öffentlichen Schlüssel PUK-BS in der Nachricht SEND aus. Auch sie merkt sich den zum öffentlichen Schlüssel PUK-BS gehörigen privaten Schlüssel PRK1-BS. Die verschlüsselt übertragenen Informationen - im vorliegenden Fall zumindest der öffentliche Schlüssel PUK-BS - kann nur von der Mobilstation MT mit Hilfe des nur ihr bekannten privaten Schlüssels PRK1-MT entschlüsselt werden. Nach dem Entschlüsseln sendet die Mobilstation MT in einer weiteren Nachricht SEND einen zweiten öffentlichen Schlüssel PUK2-MT zur Basisstation BS, die die eintreffenden Informationen - im vorliegenden Fall zumindest den zweiten öffentlichen Schlüssel PUK2-MT - mit Hilfe des nur ihr bekannten privaten Schlüssels PRK1-BS entschlüsselt. Dabei ersetzt der zweite öffentliche Schlüssel PUK2-MT den bisherigen ersten öffentlichen Schlüssel PUK1-MT. Damit ist zwischen den beiden Einrichtungen eine vertraute Verbindung („trusted re-

lationship") hergestellt, in die Dritte keinesfalls eindringen können.

Figur 3 zeigt in schematischer Darstellung den Nachrichtenfluss zur Authentifikation der in verschiedenen Kernnetzen registrierten Teilnehmer S1, S2 und zur Authentifikation des jeweiligen Kernnetzes. Dabei werden Nachrichten zwischen den die Mobilstation MT nutzenden Teilnehmern S1, S2 und der Netzeinrichtung AC, AC' (authentification center) des jeweiligen Kernnetzes transparent für das Zugangsnetz und deren Basisstation übertragen.

Zunächst sendet der Teilnehmer S1 bzw. die Mobilstation MT über die teilnehmerspezifische Einrichtung (SIM) für den Teilnehmer eine Authentifikationsanforderung aureq-mt und eine Teilnehmeridentität SID - auf Grund der teilnehmerbezogenen SIM-Karte - in der Nachricht SEND zur Einrichtung Ac des für den Teilnehmer S1 zuständigen Kernnetzes aus. Dabei erfolgt die Übertragung der Informationen verschüsselt. In der Gegenrichtung sendet die Einrichtung AC eine Authentifikationsantwort aures-co in der Nachricht SEND an die Mobilstation MT zurück, die die Authentifikationsprozedur - mit vorzugsweise geheimem Schlüssel - zur Überprüfung der Authentifikation für das Kernetz durchführt. Vorzugsweise wird gleichzeitig mit der Authentifikationsantwort aures-co eine Authentifikationsanforderung aureq-co von der Einrichtung AC des Kernnetzes verschlüsselt mitgesendet und von der Mobilstation MT empfangen. Daraufhin sendet die Mobilstation teilnehmerbezogen eine Authentifikationsantwort aures-mt in der Nachricht SEND an die Einrichtung AC verschlüsselt zurück, die die Authentifikationsprozedur zur Überprüfung der Teilnehmerauthentifikation - ebenfalls unter Verwendung vorzugsweise geheimer Schlüssel - ausführt. Eine Authentifikation nur in einer Richtung - d.h. nur für die Teilnehmer oder das Netz - ist prinzipiell auch möglich.

Der Ablauf zur Authentifikation des Teilnehmers S2 erfolgt in entsprechender Weise durch Austausch der Nachrichten SEND mit obigen Inhalten zwischen der entsprechenden teilnehmerspezifischen Einrichtung (SIM) der Mobilstation MT und der für ihn zuständigen Netzeinrichtung AC' des anderen Kernnetzes. Durch die Kombination von Verschlüsselung auf der Funkschnittstelle von/zu dem Zugangsnetz, erzielt anhand anhand mehrfach ausgetauschter öffentlicher Schlüssel auf Mobilstationsebene, und nachfolgender Authentifikation mit geheimen Schlüsseln auf Teilnehmerebene von/zu dem Kernnetz unabhängig vom Zugangsnetz wird maximale Sicherheit erreicht und dennoch bleiben Zugangsnetz - verantwortlich für Verschlüsselung - und Kernnetz(e) - verantwortlich für Authentifikation - funktional getrennt.

Patentansprüche

1. Verfahren zur Verschlüsselung von Informationen für eine Funkübertragung und zur Authentifikation von Teilnehmern (S1, S2) in einem Kommunikationssystem (UNM), das
- ein Zugangsnetz (ACN) mit Einrichtungen (BS, BSC) für die Funkübertragung sowie mindestens ein Kernnetz (CON1, CON2) mit jeweils einer Einrichtung (AC, AC') für die Teilnehmerauthentifikation aufweist,
- einen Funkkanal (RCH) zur Übertragung der Informationen über eine Funkschnittstelle(AI) von/zu mindestens einer Basisstation (BS) des Zugangsnetzes (ACN) zuteilt,

bei dem
- zwischen einer Mobilstation (MT) und der Basisstation (BS) über die Funkschnittstelle (AI) wechselseitig öffentliche Schlüssel (PUK1-MT, PUK-BS) gesendet werden,
- der von der Basisstation (BS) bzw. Mobilstation (MT) empfangene öffentliche Schlüssel (PUK1-MT bzw. PUK-BS) zur Verschlüsselung der nachfolgend über die Funkschnittstelle (AI) zu sendenden Informationen verwendet wird,
- die von der Mobilstation (MT) bzw. Basisstation (BS) empfangenen verschlüsselten Informationen anhand eines privaten Schlüssels (PRK1-MT, PRK1-BS), der dem gesendeten öffentlichen Schlüssel (PUK1-MT, PUK-BS) in der Mobilstation (MT) bzw. in der Basisstation (BS) zugeordnet ist, entschlüsselt werden, und bei dem
- von einer teilnehmerspezifischen Einrichtung (SIM) der Mobilstation (MT) die Authentifikation des jeweiligen Kernnetzes (CON1, CON2) und von der Einrichtung (AC, AC') des Kernnetzes (CON1, CON2) die Authentifikation des Teilnehmers (S1, S2) anhand wechselseitig gesendeter verschlüsselter Informationen durchgeführt werden.

2. Verfahren nach Anspruch 1, bei dem
- zunächst von der Mobilstation (MT) ein erster öffentlicher Schlüssel (PUK1-MT) zur Basisstation (BS) gesendet wird, die

ihn zur Verschlüsselung der zur Mobilstation (MT) zu sendenden Informationen verwendet,
- von der Basisstation (BS) ein öffentlicher Schlüssel (PUK-BS) zur Mobilstation (MT) gesendet wird, die ihn zur Verschlüsselung der zur Basisstation (BS) zu sendenden Informationen Informationen verwendet, und danach
- von der Mobilstation (MT) ein zweiter öffentlicher Schlüssel (PUK2-MT) zur Basisstation (BS) gesendet wird.

3. Verfahren nach Anspruch 2, bei dem
der zweite öffentliche Schlüssel (PUK2-MT) den ersten zur Basisstation (BS) gesendeten Schlüssel (PUK1-MT) ersetzt.

4. Verfahren nach Anspruch 1, bei dem
- zunächst von der Basisstation (BS) ein erster öffentlicher Schlüssel (PUK1-BS) zur Mobilstation (MT) gesendet wird, die ihn zur Verschlüsselung der zur Basisstation (BS) zu sendenden Informationen verwendet,
- von der Mobilstation (MT) ein öffentlicher Schlüssel (PUK-MT) zur Basisstation (BS) gesendet wird, die ihn zur Verschlüsselung der zur Mobilstation (MT) zu sendenden Informationen verwendet, und danach
- von der Basisstation (BS) ein zweiter öffentlicher Schlüssel (PUK2-BS) zur Mobilstation (MT) gesendet wird.

5. Verfahren nach Anspruch 4, bei dem
der zweite öffentliche Schlüssel (PUK2-BS) den ersten zur Basisstation (BS) gesendeten Schlüssel (PUK1-BS) ersetzt.

6. Verfahren nach einem der vorhergehenden Ansprüche, bei dem
- von der Mobilstation (MT) eine Teilnehmeridentität (SID) des Teilnehmers (S1, S2) und eine Authentifikationsanforderung (aureq-mt) an das Kernnetz (CON1, CON2) verschlüsselt gesendet und von der Einrichtung (AC, AC') des Kernnetzes (CON1, CON2) eine Authentifikationsantwort (aures-co) verschlüsselt rückgesendet wird,

- von der Mobilstation (MT) eine Authentifikationsprozedur zur Überprüfung der Identität des Kernnetzes (CON1, CON2) ausgeführt wird.

7. Verfahren nach Anspruch 6, bei dem
- von der Einrichtung (AC, AC') des Kernnetzes (CON1, CON2) eine Authentifikationsanforderung (aureq-co) zusätzlich zu der Authentifikationsantwort (aures-co) verschlüsselt gesendet und von der Mobilstation (MT) eine Authentifikationsantwort (aures-mt) an die Einrichtung (AC) verschlüsselt rückgesendet wird,
- von der Einrichtung (AC, AC') eine Authentifikationsprozedur zur Überprüfung der Teilnehmeridentität (SID) ausgeführt wird.

8. Verfahren nach einem der vorhergehenden Ansprüche, bei dem für die Authentifikationsprozedur geheime Schlüssel (ki) verwendet werden.

9. Verfahren nach einem der vorhergehenden Ansprüche, bei dem von dem Zugangsnetz (ACN) parallel mindestens zwei Kernnetze (CON1, CON2) bedient und ein oder mehrere Teilnehmer (S1, S2), die die Mobilstation (MT) parallel nutzen können, in verschiedenen Kernnetzen (CON1, CON2) registriert und authentifiziert werden.

10. Verfahren nach einem der Ansprüche 1 bis 8, bei dem von dem Zugangsnetz (ACN) ein Kernnetz (CON1) bedient wird, in dem mehrere Teilnehmer (S1, S2), die die Mobilstation (MT) parallel nutzen können, registriert und authentifiziert werden.

11. Verfahren nach einem der vorhergehenden Ansprüche, bei dem das Zugangsnetz (ACN) und das oder die Kernnetze (CON1, CON2) von unterschiedlichen Netzbetreibern verwaltet werden.

12. Kommunikationssystem zur Verschlüsselung von Informationen für eine Funkübertragung und zur Authentifikation von Teilnehmern (S1, S2), mit

- einem Zugangsnetz (ACN) mit Einrichtungen (BS, BSC) für die Funkübertragung sowie mindestens einem Kernnetz (CON1, CON2) mit jeweils einer Einrichtung (AC, AC') für die Teilnehmerauthentifikation,
- einem Funkkanal (RCH) zur Übertragung der Informationen über eine Funkschnittstelle (AI) von/zu mindestens einer Basisstation (BS) des Zugangsnetzes (ACN),

und mit

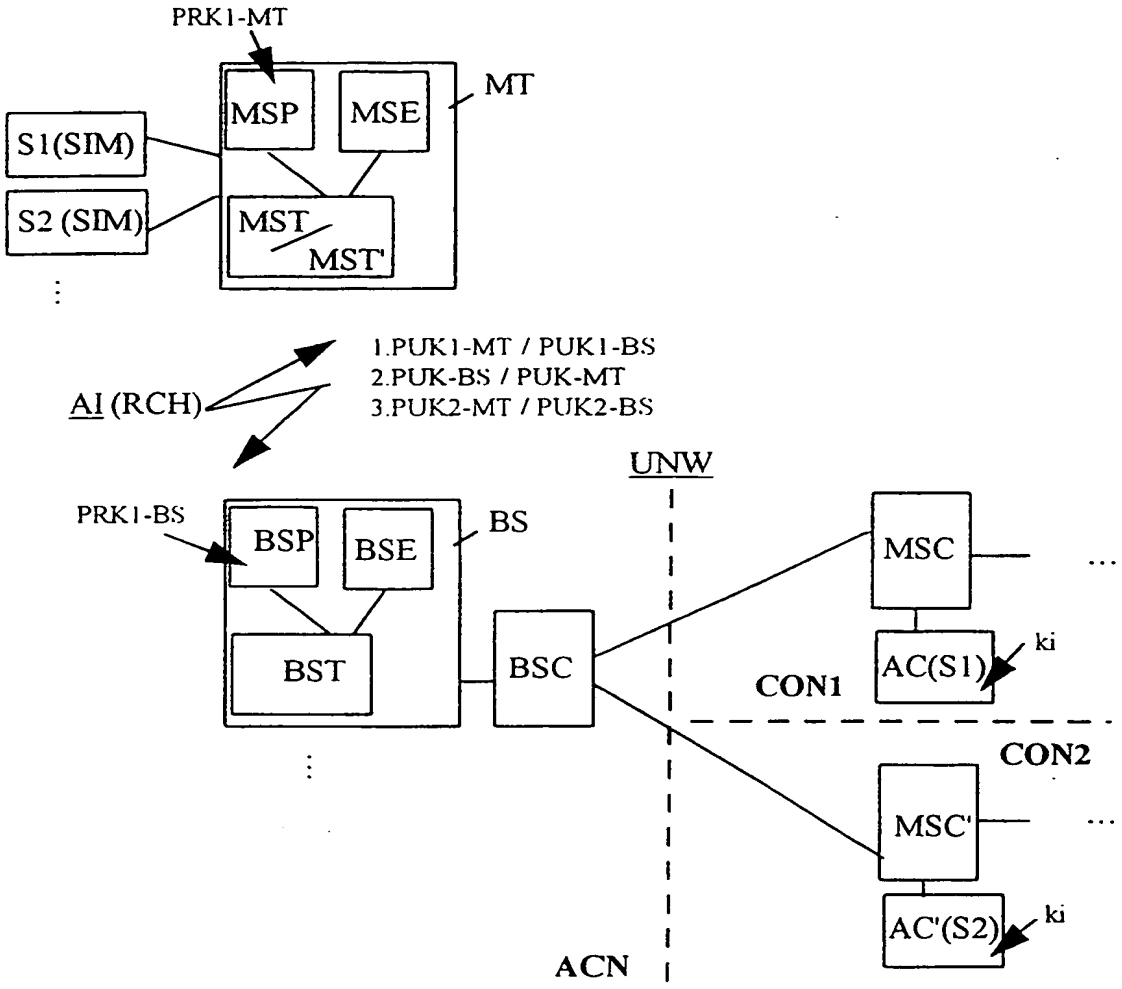
- Speichereinrichtungen (MSP, BSP) in einer Mobilstation (MT) und in der Basisstation (BS) zum Speichern öffentlicher Schlüssel (PUK1-MT, PUK-BS) und privater Schlüssel (PRK1-BS, PRK1-BS), die den öffentlichen Schlüsseln (PUK1-MT, PUK-BS) zugeordnet sind,
- Sendeeinrichtungen (MSE, BSE) in der Mobilstation (MT) und in der Basisstation (BS) zum wechselseitigen Senden der öffentlichen Schlüssel (PUK1-MT, PUK-BS) über die Funkschnittstelle (AI),
- Steuereinrichtungen (MST, BST) in der Mobilstation (MT) und in der Basisstation (BS) zur Verschlüsselung der nachfolgend über die Funkschnittstelle (AI) zu sendenden Informationen unter Verwendung der von der Basisstation (BS) bzw. Mobilstation (MT) empfangenen öffentlichen Schlüssel (PUK1-MT bzw. PUK-BS) und zur Entschlüsselung der empfangenen verschlüsselten Informationen anhand des gespeicherten zugehörigen privaten Schlüssels (PRK1-MT, PRK1-BS), und mit
- einer teilnehmerspezifischen Einrichtung (SIM) in der Mobilstation (MT) und einer Einrichtung (AC, AC') im jeweiligen Kernnetz (CON1, CON2) zur Durchführung der Authentifikation des Kernnetzes (CON1, CON2) sowie der Authentifikation der Teilnehmer (S1, S2) anhand wechselseitig gesendeter verschlüsselter Informationen.

13. Kommunikationssystem nach Anspruch 12, mit

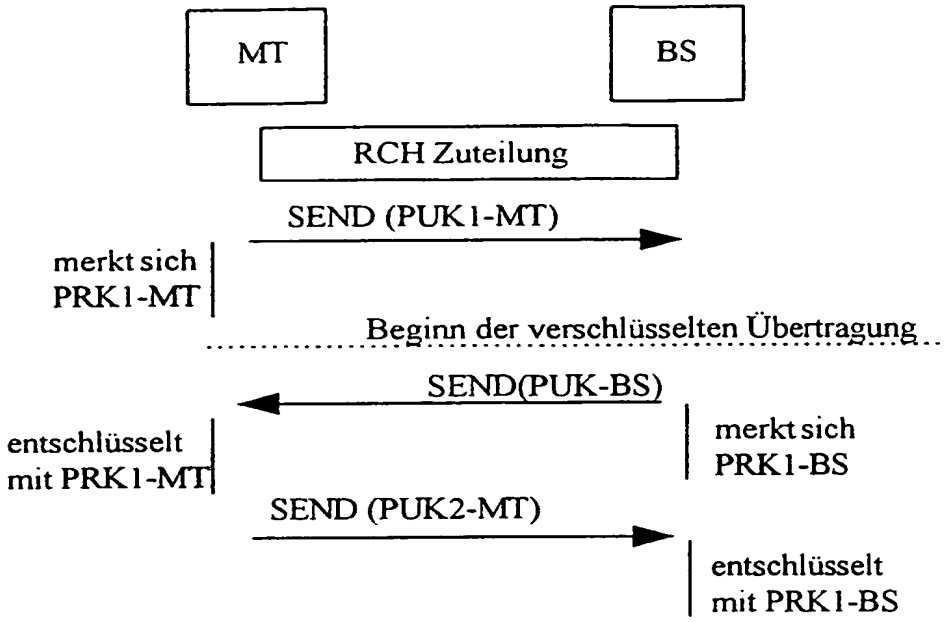
einem Zugangsnetz (ACN), an das parallel mindestens zwei Kernnetze (CON1, CON2) zur Registrierung und Authentifikation eines oder mehrerer Teilnehmer (S1, S2), die die Mobilstation (MT) parallel nutzen können, in verschiedenen Kernnetzen (CON1, CON2) angeschlossen sind.

14. Kommunikationssystem nach Anspruch 12, mit einem Zugangsnetz (ACN), an das ein Kernnetz (CON1) zur Registrierung und Authentifikation mehrerer Teilnehmer (S1, S2), die die Mobilstation (MT) parallel nutzen können, angeschlossen ist.

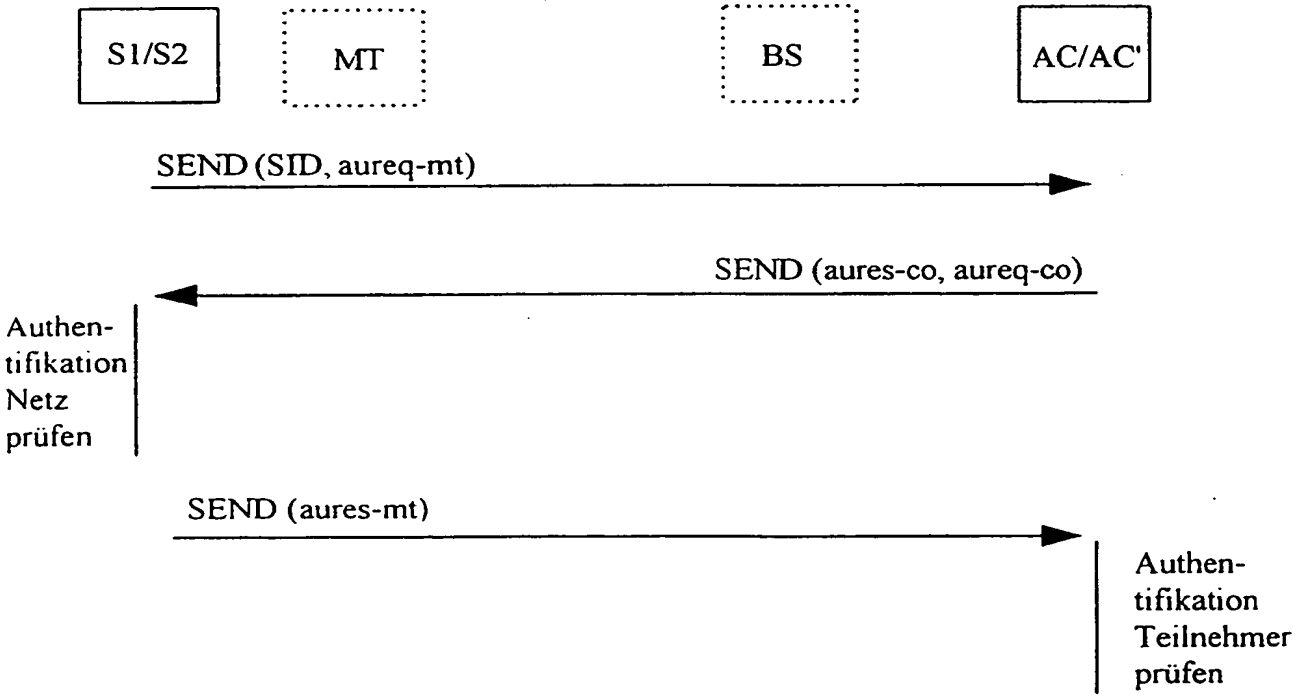
15. Kommunikationssystem nach einem der vorhergehenden Ansprüche, mit einem Zugangsnetz (ACN) und einem oder mehreren Kernnetzen (CON1, CON2), die unterschiedliche Netzbetreiber aufweisen.


PRK1-MT
MSP
MSE
MT
S1(SIM)
S2 (SIM)
MST
MST'
AI (RCH)
1.PUK1-MT / PUK1-BS
2.PUK-BS / PUK-MT
3.PUK2-MT / PUK2-BS
UNW
PRK1-BS
BSP
BSE
BS
BST
BSC
MSC
AC(S1)
ki
CON1
CON2
MSC'
AC'(S2)
ki
ACN

Figur 1



Figur 2



Figur 3

INTERNATIONAL SEARCH REPORT

Inter[illegible]pplication No
PCT/DE 98/03545

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04Q7/38

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 559 886 A (DENT PAUL W ET AL) 24 September 1996 see column 2, line 35 - column 3, line 28	1,6-8,12
A	CAMPANINI G ET AL: "PRIVACY, SECURITY AND USER IDENTIFICATION IN NEW GENERATION RADIOMOLBILE SYSTEMS" INTERNATIONAL CONFERENCE ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS,30 June 1987, pages 152-164, XP002040784 see page 154, line 15 - page 155, line 13 see page 157, line 4 - page 159, line 7	1,2,4,12

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 April 1999	12/05/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pham, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

...formation on patent family members

Inter...ial Application No
PCT/DE 98/03545

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5559886 A	24-09-1996	SE 465800 B	28-10-1991
		US 5390245 A	14-02-1995
		US 5282250 A	25-01-1994
		AT 121254 T	15-04-1995
		AU 638820 B	08-07-1993
		AU 7495291 A	10-10-1991
		CA 2051385 A	10-09-1991
		CN 1054868 A,B	25-09-1991
		DE 69108762 D	18-05-1995
		DE 69108762 T	24-08-1995
		DK 447380 T	24-07-1995
		EP 0447380 A	18-09-1991
		ES 2073726 T	16-08-1995
		FI 102134 B	15-10-1998
		HK 101895 A	30-06-1995
		IE 67887 B	01-05-1996
		JP 4505693 T	01-10-1992
		KR 144560 B	17-08-1998
		NO 300249 B	28-04-1997
		PT 96979 A,B	30-04-1993
		SE 9000856 A	10-09-1991
		WO 9114348 A	19-09-1994

INTERNATIONALER RECHERCHENBERICHT

Inte Aktenzeichen
PCT/DE 98/03545

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 H04Q7/38

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 H04Q

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 5 559 886 A (DENT PAUL W ET AL) 24. September 1996 siehe Spalte 2, Zeile 35 - Spalte 3, Zeile 28 ---	1,6-8,12
A	CAMPANINI G ET AL: "PRIVACY, SECURITY AND USER IDENTIFICATION IN NEW GENERATION RADIOMOLBILE SYSTEMS" INTERNATIONAL CONFERENCE ON DIGITAL LAND MOBILE RADIO COMMUNICATIONS,30. Juni 1987, Seiten 152-164, XP002040784 siehe Seite 154, Zeile 15 - Seite 155, Zeile 13 siehe Seite 157, Zeile 4 - Seite 159, Zeile 7 -----	1,2,4,12

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
29. April 1999	12/05/1999

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Pham, P

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen
PCT/DE 98/03545

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5559886 A	24-09-1996	SE	465800 B	28-10-1991
		US	5390245 A	14-02-1995
		US	5282250 A	25-01-1994
		AT	121254 T	15-04-1995
		AU	638820 B	08-07-1993
		AU	7495291 A	10-10-1991
		CA	2051385 A	10-09-1991
		CN	1054868 A,B	25-09-1991
		DE	69108762 D	18-05-1995
		DE	69108762 T	24-08-1995
		DK	447380 T	24-07-1995
		EP	0447380 A	18-09-1991
		ES	2073726 T	16-08-1995
		FI	102134 B	15-10-1998
		HK	101895 A	30-06-1995
		IE	67887 B	01-05-1996
		JP	4505693 T	01-10-1992
		KR	144560 B	17-08-1998
		NO	300249 B	28-04-1997
		PT	96979 A,B	30-04-1993
		SE	9000856 A	10-09-1991
		WO	9114348 A	19-09-1994